FIPS-COMPLIANT ENCRYPTION SYSTEM WITH QUANTUM KEY DISTRIBUTION

Fi ld of the Invention

The present invention relates to encryption systems and methods that satisfy the Federal Information Processing Standard (FIPS), and more particularly relates to such systems and methods that utilize quantum key distribution (QKD).

Background of the Invention

Federal Information Processing Standards (FIPS)

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for government-wide use. NIST develops FIPS when there are compelling Federal government requirements, such as for security and interoperability, and there are no acceptable industry standards.

The FIPS governing the security requirements for cryptographic equipment ("modules") is set forth in FIPS Publication 140-2. This standard specifies the security requirements that need to be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The standard provides for increasing qualitative levels of security ranked as Levels 1 through 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of cryptographic module ports and interfaces, roles, services and authentication, finite state models, physical security, operation environment, cryptographic key management, electromagnetic interference/compatibility (EMI/EMC), self tests; design assurance, etc.

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to the FIPS 140-2 standard, as well as to other cryptography-based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Canadian Government. Products validated as conforming to the FIPS 140-2 standard are accepted by the Federal agencies of the U.S. and Canada for protecting "sensitive information" (U.S.) or "designated information" (Canada). The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

In the CMVP, vendors of cryptographic modules use independent accredited testing laboratories (e.g., Atlan Laboratories, McLean, Virginia) to have their modules tested. National Voluntary Accreditation Program (NVLAP) accredited laboratories perform cryptographic module compliance/conformance testing.

Though FIPS are ostensibly for the procurement of equipment by the government, the practical effect is that private industry also looks to the FIPS standards when purchasing equipment. This is, in part, because NIST collaborates with national and international standards committees, users, industry groups, consortia and research and trade organizations to develop the standards. Thus, it is to a company's business advantage that their equipment satisfy FIPS even if it has no intention of selling equipment to the government.

Virtual Private Networks (VPNs)

A virtual private network (VPN) is a secure private network connection built on top of a publicly accessible communication structure, such as the Internet or the public telephone network. For security reasons, data sent over a VPN is typically encrypted. Further, other measures such as digital certificates, access control, and strong user authentication are employed to enhance system security. Prior to VPNs, users had to contact one another by establishing

computer connections via dial-up over telephone lines into a remote access server (RAS).

FIG. 1 is a schematic diagram of a prior art commercially available FIPS-compliant encrypted VPN 20 that links two parties, Alice and Bob. VPN 20 includes two encryption/decryption (e/d) processors 24 and 26. Alice is connected to e/d processor 24 via an Ethernet section 30. Bob is connected to e/d processor 26 via an Ethernet section 32. The e/d processors 24 and 26 are connected via a VPN link 40 (e.g., the Internet).

In the operation of VPN 20, Alice transmits a plaintext signal 50 over Ethernet link 30 to e/d processor 24. Plaintext signal 50 is encrypted at e/d processor 24 to form an encrypted signal 54, which is transmitted over VPN link 40 to e/d processor 26, where it is decrypted and converted back into a plaintext signal 50'. Plaintext signal 50' then travels from e/d processor 26 over Ethernet link 32, and is received by Bob.

An example of a FIPS-compliant VPN 20 is the DiamondTeck™ VPN, available from Cryptek, Inc., Sterling, VA.

QKD and Link Encryption

FIG. 2 is a schematic diagram of a prior art VPN 100 for performing encrypted communication between Alice and Bob using QKD. VPN 100 includes two encryption/decryption (e/d) processors 106 and 110. Alice is connected to e/d processor 106 via Ethernet section 116. Bob is connected to e/d processor 110 via Ethernet section 120. The e/d processors 106 and 110 are connected via VPN link 130.

Included in VPN 100 is a QKD system 150 having a quantum channel 156 connecting two QKD stations 160 and 164. The QKD station 160 is connected to e/d processor 106 via a connection 170, and QKD station 164 is connected to e/d processor 110 via a connection 172.

In the operation of VPN 100, a quantum key 178 is securely exchanged between QKD stations 160 and 164 using any one of a number of known quantum cryptographic methods. Once the key is securely exchanged, it is

distributed to e/d processors 106 and 110 via signals 180 and 184 from QKD stations 160 and 164, respectively. This is referred to as symmetric key distribution. The quantum key is then used to encrypt a plaintext Ethernet signal 200 from Alice at e/d processor 106 to form encrypted signal 202 and send it over VPN link 130, where it is decrypted at e/d processor 110 to form decrypted signal 200', which is sent to Bob over Ethernet section 130.

FIPS and QKD Encryption Systems

System 100 of FIG. 2 is not FIPS compliant by definition because such standards have not yet been developed for the nascent field of quantum cryptography. It is anticipated that establishing such standards will take many years. This is a major problem for companies that seek to enter the cryptography market and sell QKD-based encryption systems since, as mentioned above, both government and non-government organizations look to FIPS as a governmental "seal of approval" when making purchasing decisions.

Summary of the Invention

A first aspect of the invention is a FIPS-complaint QKD-based encryption system. The system includes a FIPS-compliant VPN layer, a classical encryption layer operatively connected to the FIPS-compliant VPN layer, and a QKD layer operatively connected to the classical encryption layer. The QKD layer provides a quantum key to the classical encryption layer so that the classical encryption layer is capable of encrypting information from the FIPS-compliant VPN layer using the quantum key.

A second aspect of the invention is a method of forming a FIPS-compliant QKD encryption system using a FIPS-compliant VPN. The method includes forming a classical encryption link by operatively connecting first and second operatively connected encryption/decryption (e/d) processors to respective first and second VPN stations of the FIPS-compliant VPN. The method further includes operatively connecting first and second operatively connected QKD stations of a QKD system to the first and second e/d processors, respectively,

wherein the first and second QKD stations are capable of exchanging a quantum key and providing the quantum key to the first and second e/d processors.

A third aspect of the invention is a method of transmitting an encrypted signal between first and second transmitting/receiving stations. The method includes sending a first plaintext signal from the first transmitting/receiving station to a first VPN station of a FIPS-compliant VPN, and converting the first plaintext signal to a first VPN signal at the first VPN station. The method further includes providing the first VPN signal to a first encryption/decryption (e/d) processor of a classical encryption system also having a second e/d processor, and exchanging a quantum key between first and second QKD stations in a QKD system, and then providing the quantum key to the first and second e/d processors. The method also includes forming an encrypted VPN signal from the first VPN signal at the first e/d processor using the quantum key provided to the first e/d processor, and forming a decrypted VPN signal from the encrypted VPN signal at the second e/d using the quantum key provided to the second e/d processor. The method further includes forming a second plaintext signal from the decrypted VPN signal at a second VPN station in the VPN, and receiving the second plaintext signal at the second transmitting/receiving station.

Brief Description of the Drawings

FIG. 1 is schematic diagram of a prior art FIPS-compliant encryption system as implemented on a VPN;

FIG. 2 is a schematic diagram of a prior art encryption system that employs symmetric quantum key distribution to distribute a quantum key and send an encrypted signal over a VPN, and that is not FIPS compliant; and

FIG. 3 is a schematic diagram of the FIPS-compliant QKD-based encryption system of the present invention for sending encrypted signals over a VPN.

Detailed Description of the Invention

FIG. 3 is a schematic diagram of the FIPS-compliant QKD-based encryption system 300 of the present invention. System 300 is capable of sending encrypted signals over a VPN between first and second transmitting/receiving stations, referred to as Alice and Bob, respectively.

System 300 includes a FIPS-compliant VPN encryption system 302 similar to system 20 illustrated in FIG. 1, and which includes VPN stations 304 and 306. Stations 304 and 306 may be, for example, two computers. Alice is connected to VPN station 304 via link 310. Bob is connected to VPN station 306 via link 312. In an example embodiment, links 310 and 312 are Ethernet links.

System 300 also includes a classical encryption system 314 that includes e/d processors 106 and 110. VPN station 304 is operatively connected to e/d processor 106 via VPN link 320 and VPN station 306 is operatively connected to e/d processor 110 via VPN link 324. The e/d processors 106 and 110 are operatively connected to one another via VPN link 130, as in FIG. 2. VPN links 320, 324 and/or 130 can be any one of a number of network-type links, such as those associated with a local area network (LAN), a metropolitan area network (MAN), wide area network (WAN), Internet, Intranet, Ethernet or public switched telephone network (PSTN).

In an example embodiment, e/d processors 106 and 100 each include a quantum key storage device 328 capable of storing quantum keys. An example quantum key storage device 328 includes non-volatile memory and circuitry sufficient to store and retrieve the quantum keys. In a preferred example embodiment, e/d processors 106 and 110 are included within VPN stations 304 and 306, respectively.

Classical encryption system 314 is, for example, a link encryptor. An example link encryptor is available from GDS, Inc. (Switzerland).

Also included as part of system 300 is the QKD system 150 of FIG. 2. QKD system 150 includes quantum channel 156 connecting the two QKD stations 160 and 164. QKD station 160 is operatively connected to e/d processor

106 via a connection 170, and QKD station 164 is operatively connected to e/d processor 110 via a connection 172.

Thus, system 300 includes three different operatively interconnected layers, identified in FIG. 3 as Layers I, II and III. The three layers are hierarchically distinguished in FIG. 3 by dashed lines 350 and 360. Layer I is the FIPS-compliant VPN layer, Layer II is the classical encryption layer, and Layer III is the QKD layer. Layers I-III are hierarchically arranged so that Layer I is the "highest" or uppermost level and Layer II is the "lowest" or bottom level.

In the operation of system 300, in Layer I Alice transmits a plaintext signal 50 over Ethernet section 30 to VPN station 304. Here, a "plaintext signal" means any non-encrypted signal, and is also referred to below and in the claims more generally as "information." VPN station 304 receives plaintext signal 50 and converts plan text signal 50 to a VPN signal 380. Here, a "VPN signal" is any signal that travels over the VPN. Signal 380 is then transmitted to e/d processor 106 residing in Layer II.

Prior to, afterwards, or in synchrony therewith, in Layer III quantum key 178 is securely exchanged between QKD stations 160 and 164 using any one of a number of known quantum cryptographic methods. Once the key is securely exchanged (i.e., "quantum exchanged"), it is symmetrically distributed to e/d processors 106 and 110 via signals 180 and 184 from QKD stations 160 and 164, respectively. In an example embodiment of system 300, e/d processors 106 and 110 are included within QKD stations 160 and 164, respectively, for enhanced security.

VPN signal 380 is passed to e/d processors 106 and 110, where the signal is encrypted by a symmetric key encryption algorithm to form an encrypted signal 400. Examples of symmetric key encryption algorithms include AES or TDES that operate in a mode of operation approved by NIST, such as electronic codebook, cipher block chaining, cipher feedback, output feedback, counter mode, or one time pad encryption. VPN stations 304 and 306 also provide message authentication and data integrity functionality. If needed, e/d processors 106 and 110 can provide full functionality of a secure link, i.e., not just

encryption/decryption. For example, e/d processors 106 and 110 can also add message authentication, and data packet control functionality on the top of VPN signal 380 when forming signal 400. Message authentication is accomplished, for example, by adding MAC values to signal 400 (e.g., in the form of data packets) sent over link 130. For that purpose, any known secure message authentication algorithm can be used (e.g., HMAC SHA-1).

The e/d processors 106 and 110 can also add headers with data packet numbers, etc., to signal 400. As mentioned above, the keys for e/d processors 106 and 110 are provided by the QKD apparatus (Layer III). The e/d processors 106 and 110 include a key management method (protocol) that synchronizes the keys in each e/d processor and that performs key refreshing at select time intervals. For example, the (quantum) keys coming from QKD stations 160 and 164 (via signals 180 and 184) are split into two tables, one for each direction of communication. In an example embodiment, two more tables may be created for authentication. Each table contains, for example, a key ID, timestamp, or other information. The key ID (as well as some additional information) is then sent over channel 130 unencrypted as a signal 402, together with the encrypted signal (packet) 400, to provide key synchronization and refreshing functionality.

In this manner then, the e/d processors 106 and 110 are "interfaced" (i.e., operatively connected) to QKD stations 160 and 164, and to VPN stations 304 and 306.

Once the quantum key is distributed to e/d processors 106 and 110, it is used in Level II to classically encrypt VPN signal 380 at e/d processor 106 to form encrypted signal 400, as discussed above. This signal travels over Ethernet section 130 to e/d processor 110. At e/d processor 110, encrypted signal 400 is decrypted using the quantum key provided to e/d processor 110, thereby forming decrypted VPN signal 380', which in turn is sent to VPN station 306. VPN station 306 converts VPN signal 380' to a plaintext Ethernet signal 50' and sends it to Bob over Ethernet section 312.

Because system 300 includes a FIPS-compliant VPN as Layer I and a classic encryption system in Layer II (which may also be FIPS-compliant, but is

need not be), system 300 as a whole is FIPS-compliant. The QKD system in Layer III operates transparently beneath FIPS-compliant Layer I and (optionally FIPS-compliant) layer II. Nevertheless, Layer III provides system 300 with enhanced security as compared to the having only the classical encryption layer because the quantum transmission of the key. It is important to note that the presence of QKD Layer III does not render the system as a whole FIPS-noncompliant because it only serves to enhance the security of the system.

While the present invention has been described in connection with preferred embodiments, it will be understood that it is not so limited. On the contrary, it is intended to cover all alternatives, modifications and equivalents as may be included within the spirit and scope of the invention as defined in the appended claims.